View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by ePrints.FRI

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Jure Janša

Merjenje zmogljivosti in optimizacija navideznih naprav DataPower

DIPLOMSKO DELO

UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Jure Janša

Merjenje zmogljivosti in optimizacija navideznih naprav DataPower

DIPLOMSKO DELO

UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

MENTOR: doc. dr. Miha Moškon

Ljubljana, 2014

To delo je ponujeno pod licenco *Creative Commons Priznanje avtorstva-Deljenje pod enakimi pogoji 2.5 Slovenija* (ali novejšo različico). To pomeni, da se tako besedilo, slike, grafi in druge sestavine dela kot tudi rezultati diplomskega dela lahko prosto distribuirajo, reproducirajo, uporabljajo, priobčujejo javnosti in predelujejo, pod pogojem, da se jasno in vidno navede avtorja in naslov tega dela in da se v primeru spremembe, preoblikovanja ali uporabe tega dela v svojem delu, lahko distribuira predelava le pod licenco, ki je enaka tej. Podrobnosti licence so dostopne na spletni strani creativecommons.si ali na Inštitutu za intelektualno lastnino, Streliška 1, 1000 Ljubljana.

Izvorna koda diplomskega dela, njeni rezultati in v ta namen razvita programska oprema je ponujena pod licenco *GNU General Public License*, različica 3 (ali novejša). To pomeni, da se lahko prosto distribuira in/ali predeluje pod njenimi pogoji. Podrobnosti licence so dostopne na spletni strani http://www.gnu.org/licenses. [1]

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Kandidat naj v diplomskem delu opiše delovanje in ponudbo fizičnih in navideznih DataPower naprav s strani podjetja IBM. Izvede naj konfiguracijo testnega okolja in v njem primerja delovanje fizičnih in navideznih naprav. V izsledkih dela naj poda vodila pri izbiri in konfiguraciji ustreznih navideznih naprav v ciljnem okolju.

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani Jure Janša, z vpisno številko **63030118**, sem avtor diplomskega dela z naslovom:

Merjenje zmogljivosti in optimizacija navideznih naprav DataPower

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Miha Moškona
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 19. september 2014 Podpis avtorja:

Zahvaljujem se doc. dr. Mihi Moškonu za strokovno pomoč in usmerjanje pri pripravi diplomske naloge. Prav tako se zahvaljujem tudi vsem drugim, ki so mi pomagali pri dokončanju študija, posebno Nisi in Manci.

Kazalo

Seznam uporabljenih kratic

Kratica	angleško	slovensko
XML	Extensible Markup Language	Razširljivi označevalni jezik
SOAP	Simple Object Access protocol	Protokol za spletne storitve
SOA	Service-oriented architecture	Storitveno usmerjena arhitektura
ESB	Enterprise service bus	Visoko zmogljivo storitveno vodilo
XPath	XML Path Language	XML poizvedovalni jezik
XSD	XML Schema definition	Definicija XML-sheme
XKMS	XML Key Management Specification	Specifikacije za upravljanje XML
XSL	Extensible Stylesheet Language	Družina jezikov za oblikovanje, preoblikovanje in prikazovanje XML
XSLT	Extensible Stylesheet Language Transformations	Transformacije za XSL
SAML	Security Assertion Markup Language	Varnostno označevalni jezik
HTTP	Hypertext Transfer Protocol	Protokol za prenos hiperteksta
HTTPS	Hypertext Transfer Protocol Secure	Varni protokol za prenos hiperteksta
MQ	Message Oriented Middleware	Sporočilno vmesno programje
FTP	File transfer protocol	Protokol za prenos datotek
SFTP	Secure file transfer protocol	Varni protokol za prenos datotek
COBOL	Compiled computer programming language	Prvotno nestrukturiran programski jezik
GUI	Graphical user interface	Grafični uporabniški vmesnik

DMZ	Demilitarized zone	Demilitarizirano območje
XDoS	XML denial-of-service attack	XML-ohromitev storitve
X.509	Public key infrastructure	Infrastruktura javnih ključev
SSL	Secure socket layer	Sloj varnih vtičnic
LDAP	Lightweight Directory Access Protocol	Internetni protokol za dostop do imenikov
URL	Uniform resource locator	Enolični krajevnik vira
URI	Uniform resource identifier	Enolični označevalnik vira
SQL	Structured query language	Strukturiran povpraševalni jezik
SNMP	Simple network management protocol	Protokol za upravljanje naprav v omrežju
SLM	Service level management	Upravljanje ravni storitve
WSDM	Web Services Distributed Management	Porazdeljeno upravljanje spletnih storitev
UDDI	Universal Description, Discovery and Integration	XML-register
WSDL	Web Services Description Language	Jezik za opis spletnih storitev
ASN.1	Abstract Syntax Notation One	Abstraktna notacija
CSV	Comma separated value	Običajni format za besedilno datoteko
ebXML	Electronic Business using XML	Poslovni XML
HSM	Hardware security module	Strojno varnostni modul
CLI	Command-line interface	Vmesnik z ukazno vrstico
NTP	Network Time Protocol	Omrežni protokol za čas
WAF	Web application firewall	Požarni zid za spletne aplikacije
MPGW	Multi-protocol gateway	Večprotokolni prehod
WSP	Web service proxy	Posredovalni strežnik za spletne storitve
WSRR	WebSphere Service Registry and Repository	WebSphere register za spletne storitve

JMS	Java messaging service	Storitev za asinhrono izmenjavo podatkov
AAA	Authentication, authorization and accounting	Overitev, pooblastitev in računovodstvo
SLA	Service level agreement	Dogovor o ravni storitve
DoS	Denial of service	Ohromitev storitve
IT	Information technology	Informacijska tehnologija
OSI	Open systems interconnection	Referenčni model za razvoj in oblikovanje komunikacijskih protokolov in protokolov računalniških omrežij
IP	Internet protocol	Internetni protokol
RADIUS	Remote Authentication Dial In User Service	Protokol za centraliziran AAA
WS	Web service	Spletna storitev
NFS	Network file system	Omrežni datotečni sistem
FIPS	Federal Information Processing Standards	Varnostni in komunikacijski standard
SSH	Secure shell	Varna lupina
DVD	Digital versatile disc	Digitalna prilagodljiva plošča

Povzetek

V diplomskem delu opišemo delovanje in ponudbo fizičnih in navideznih naprav DataPower s strani podjetja IBM. Predstavimo kako so nam lahko namenske naprave DataPower v pomoč v SOA (*angl. Service Oriented Architecture*) okoljih. Opišemo vzpostavitev testnega okolja in testiranje z uporabo fizičnih naprav XI50 in XI52 ter navidezne naprave z različnimi konfiguracijami. Na koncu analiziramo zajete podatke in v izsledkih dela podamo vodila pri izbiri in konfiguraciji ustreznih navideznih naprav v ciljnem okolju.

Ključne besede: naprava DataPower, navidezna naprava, merjenje zmogljivosti, optimizacija, SOA

Abstract

Thesis describes the market of IBM DataPower appliances and their corresponding functionalities. We explain the benefits of these devices in the SOA (Services Oriented Architecture) environments. Case study of testing environment configuration is demonstrated on the physical XI50 and XI52 models and various configurations of virtual DataPower appliance. The analysis of the data obtained with these configurations is performed. At the end we provide the principles and guidelines for the proper configuration of virtual DataPower appliances in target environment.

Keywords: DataPower appliance, virtual machine, performance test, optimization, SOA

Poglavje 1 Uvod

Z razširitvijo XML in spletnih storitev smo doživeli eksplozijo v razvoju vmesne infrastrukture računalniških omrežij (angl. *middleware*). Zelo pomembna komponenta v XML-arhitekturi je ESB. Predstavlja skupino komponent, ki nam omogoča komunikacijo med storitvami, kot so usmerjanje, transformacije, upravljanje, varnost in podobne funkcije.

1.1 Opis problema

XML in SOAP omogočata univerzalno komunikacijo med storitvami v ljudem prijazni obliki. Večanje velikosti in kompleksnosti tradicionalnih namestitev vmesnih programov posledično pomeni večje stroške povezane z namestitvijo in upravljanjem SOA-okolij. Razčlenjevanje in obdelava podatkov negativno vplivata na zmogljivosti celotnega sistema. Večina rešitev to odpravi z dodajanjem dodatnih virov, kar pa pripelje do povečanja stroškov (strojna oprema, licence itd.). Z novo tehnologijo so prišle nove težave. Pojavile so se nove oblike napadov in varnostnih lukenj na sistemih, ki uporabljajo arhitekturo zasnovano na vmesni infrastrukturi. Namenske naprave DataPower bistveno olajšajo premagovanje omenjenih izzivov.

1.2 Cilj diplomskega dela

Do nedavnega je bila naprava DataPower (XG45 in XI52) na voljo samo v fizični obliki. S pojavom navidezne naprave XG45 in XI52 smo dobili nove možnosti za postavitev vmesne infrastrukture. Navidezne naprave omogočajo iste funkcionalnosti kot fizične naprave. Zelo pomemben korak pri namestitvi navidezne naprave je načrtovanje potrebnih virov za procesiranje podatkovnega toka. Posebno pozorni moramo biti na trenutke povečane obremenitve (angl. *peak intervals*). Za razliko od fizičnih naprav moramo pri navidezni napravi vire nastaviti na hipernadzorniku. Cilj diplomskega dela je vzpostavitev metodologije in oblikovanje dokumenta, ki nam bo v pomoč pri načrtovanju namestitve navidezne naprave v različna okolja.

1.3 Členitev dela

V poglavju 2 opišemo različne izvedbe naprave DataPower. Predstavimo njihovo običajno uporabo, storitve in delovanje. Poglavje 3 opiše testno okolje, konfiguracijo MPGW in način zajemanja podatkov. V poglavju 4 so navedeni testni scenariji, analizirani zajeti podatki in podana splošna priporočila za konfiguracijo navidezne naprave.

Poglavje 2 Predstavitev naprave DataPower

Naprave DataPower so zelo vsestranske in jih lahko uporabimo za reševanje različnih problemov v SOA-okoljih [1, 2]. Tehnična osnova SOA je podpora za XML in spletne storitve. Z uporabo SOAP-standarda lahko SOA-odjemalec pokliče storitev brez podpore velikega števila različnih protokolov in oblik sporočil. Z uporabo SOAP-vmesnika storitve spremenimo v navidezne in s tem odpravimo potrebo po poznavanju podrobnosti o sami implementaciji.

Uporaba XML omogoča, da so podatki z eksplicitno jezikovno podporo za običajne operacije, ki nam omogočajo njihovo obdelavo, samozadostni. Z uporabo XPath jezika lahko na dosleden način izberemo podatke iz XML-dokumenta. Posredniki storitev lahko XML-podatke uporabijo za usmerjanje podatkovnega toka, kontrolo varnosti, obdelavo podatkov v zahtevi in v odgovoru, ločeno od same implementacije storitve.

Uporaba rahlo povezanih, navideznih storitev v SOA-okoljih ima določeno ceno, na primer potreba po dodatnih licencah. Zaradi vse večje kompleksnosti XML- in SOA-operacij je običajna vmesna programska oprema začela zaostajati. To je seveda privedlo do novih izzivov, npr. zagotavljanje varnosti v primeru škodljivih XML-sporočil.

2.1 Opis naprave

Družina DataPower vsebuje namenske omrežne naprave, ki nam pomagajo premagati marsikatero težavo, s katero se soočamo v SOA- in XML-svetu. Z uporabo naprave DataPower lahko razbremenimo spletne in aplikacijske strežnike, s procesiranjem XML, XSD, Xpath in XSLT s hitrostjo omrežja. Naprave DataPower ponujajo naslednje funkcionalnosti:

- Naprave omogočajo XML/SOAP požarni zid, zagotavljajo XML-varnost, preverjanje podatkov, kontrolo dostopa do spletnih storitev in navideznost spletnih storitev.
- Posredovanje sporočil je neodvisno od protokolov, vgrajena je varnost na nivoju sporočila, naprave imajo zelo razčlenjeno kontrolo dostopa in zmožnost povezovanja različnih omrežij.

- Visoka zmogljivost je dosežena z več stopenjskim procesiranjem s hitrostjo omrežja (angl. *wire-speed*), vključno z XML, XSLT, XPath in XML preverjanjem shem.
- Ponujajo centralizirano politiko za storitve in upravljanje na nivoju storitve.
- Podpirajo različne varnostne protokole, kot so WS-Security, SAML 1.0/1.1/2.0, WS-Federation, WS-Trust, XKMS, Radius itd.
- Podpirajo različne transportne protokole, kot so HTTP/HTTPS, MQ, FTP, SFPT itd.
- Omogočajo pretvorbo med različnimi oblikami podatkov, npr. binarno v XML, COBOL v XML.

Naprave DataPower lahko pomagajo pri ovirah, ki se pojavljajo v SOA-omrežjih:

- Sama namestitev in upravljanje sta zelo preprosta, poleg tega nudijo podporo za uveljavljene in prihajajoče standarde.
- Z njimi dosežemo SSL-pospešitve, razbremenitev preobremenjenih strežnikov (XML-procesiranje, pretvorba različnih oblik podatkov).

2.1.1 DataPower XML Security Gateway XG45

Naprava omogoča varnostno in izvršilno točko za XML-transakcije in spletne storitve. Nastavimo lahko šifriranje, požarni zid, digitalni podpis, preverjanje shem, WS-Security, XML-kontrolo dostopa in Xpath. Zato je XG45 zelo primerna naprava za v DMZ.

Model XG45 ponuja še naslednje:

- XML/SOAP-požarni zid: XML Security Gateway XG45 filtrira podatke pri hitrosti omrežja na podlagi informacij od drugega do sedmega nivoja po OSI-modelu. Filtrira promet na ravni polja sporočila in SOAP-ovojnice do IP-naslova, vhoda ali imena gostitelja, velikosti podatkov itd. Filtri so lahko prednastavljeni s pomočjo prijaznega GUI Xpath-vmesnika in avtomatsko naloženi. Z njimi spreminjamo varnostno politiko na osnovi ure v dnevu ali drugih sprožilcev.
- XML/SOAP-preverjanje sheme: Naprava ima edinstveno sposobnost preverjanja XML-sheme in sporočila, s čimer zagotovimo, da so zahteve in odgovori pravilno strukturirani in zaščiteni pred nevarnostmi, kot so na primer XDoS-napadi, napolnitev medpomnilnika, namerno in nenamerno deformirani XML-dokumenti.

- Varnost na osnovi polja v sporočilu: Model XG45 selektivno deli informacije z uporabo šifriranja oziroma dešifriranja, digitalnega podpisa oziroma preverjanja podpisa celotnega XML-sporočila ali dela XML-sporočila. Razdeljena in dinamična varnostna politika lahko temelji na katerikoli spremenljivki, npr: vsebina sporočila, IP-naslov, ime gostitelja ali drugi uporabnikovi filtri.

- Kontrola dostopa: XG45 podpira veliko mehanizmov za preverjanje dostopa WS-Security, WS-Trust, X.509, SAML, SSL; LDAP, RADIUS in tudi preprosto URL-mapiranje. Lahko preverja pristopne pravice z zavrnitvijo nepodpisanih sporočil ali pa iskanje podpisa znotraj SAML.

- Navideznost storitev: XML-spletne storitve od podjetij zahtevajo, da izpostavijo svoje vire, ne da bi podali informacije o lokaciji in konfiguraciji. S kombinacijo URL-prepisov, visoko zmogljivih XSLT-transformacij in XML/SOAP-usmerjanja lahko transparentno povežejo storitve na svoje zaledne sisteme.

- Centralna polika upravljanja: Napravo z lahkoto vključimo v obstoječa okolja. Podjetja tako centralizirajo varnostne funkcije, jih tudi posodobijo ter tako zmanjšajo stroške. Funkcionalnost, kot je požarni zid, preko GUI v zelo kratkem času lahko preprosto konfiguriramo. Z uporabo XSLT lahko naredimo zelo prefinjeno varnostno politiko in pravila za usmerjanje. Napravo upravljamo lokalno ali preko oddaljenega dostopa. Naprava podpira SNMP, skriptne jezike in beleženje dogodkov na oddaljeni sistem.

- SLM: Naprava podpira WSDM, UDDI, WSDL, dinamično odkrivanje in omogoča različne SLM konfiguracije. Tako robustna podpora omogoča zelo učinkovito upravljanje SOA okolij.

- Transformacija med različnimi formati: Spreminjamo lahko podatke iz in v binarno obliko, navaden tekst, XML, COBOL, CSV, ASN.1 in ebXML. Za razliko od prilagojenih rešitev patentirana tehnologija DataGlue ponuja v naprej pripravljeno rešitev.

- Povezovanje: Omogoča povezovanje zahtev in odgovorov med različnimi protokoli, HTTP, HTTPS, MQ, FTP, SFTP itd.

2.1.2 DataPower Integration Appliance XI52

Pravi opis za XI52 bi bil strojni ESB. Tudi XG45 lahko opravlja isto funkcijo, samo v manjši kapaciteti. Vsebuje vse kar ima XG45. Glavne razlike so v večjem pomnilniku, večjem številu

omrežnih vhodov, večji diskovni kapaciteti. Zaradi teh zmožnosti jo običajno najdemo v zasebnem omrežju kjer opravlja nalogo ESB, seveda lahko napravo uporabimo tudi v DMZ.

Obstajajo še specializirane naprave, kot sta XB62 B2B in XC10 Caching, ki pa sta izven obsega predstavitve tega dela.

2.1.3 DataPower Integration Appliance XI50

Je predhodnica naprave XI52 z istimi funkcionalnostmi. Razlika je v virih, ki so ji na voljo. Na voljo ima manjšo količino pomnilnika, omrežnih kartic in diskovne kapacitete.

2.1.4 Navidezna naprava DataPower

Navidezna različica naprav DataPower nam omogoča iste funkcionalnosti kot fizična naprava. Navidezna verzija je narejena na osnovi navidezne naprave na namensko narejeni platformi z vgrajenim optimiziranim operacijskim sistemov.

Oglejmo si razlike na visoki ravni. Prednosti fizične naprave so sledeče:

- Fizična naprava ima strojno zaščito pred nedovoljenim vstopom in namernim spreminjanjem samega fizičnega sistema. Naprava ima senzorje za detekcijo nedovoljenega dostopa. Narejena je tudi veriga zaupanja do strojnega nivoja z uporabo Trusted Platform module čipa. Navidezna naprava DataPower je razvita z isto varnostno politiko kot fizična naprava, toda brez strojne zaščite. Navidezna naprava se mora zanesti na varnost, ki jo omogočata uporabljena strojna oprema in hipernadzornik.

- Fizične naprave DataPower so FIPS 140-2 stopnja 3 certificirane kadar uporabljajo opcijski strojno varnostni modul (HSM). HSM je že tovarniško vgrajen v napravo. Z njim dosežemo, da imamo nedostopno shrambo za zasebne ključe, s katerimi izvajamo šifrirne operacije.

- Namensko narejena fizična naprava ima strojno pospešene operacije, npr. šifriranje.

Prednosti navideznih naprav so:

- Navidezno napravo lahko namestimo na različno strojno opremo. Nameščena je lahko v zasebni ali javni oblak. Navidezne naprave z lahkoto premestimo iz enega strežnika na drugega. V primeru rasti okolja z lahkoto dodajamo nove naprave in povečujemo zmogljivost obstoječih.

- Neprodukcijska verzija navidezne naprave nam omogoča postavitev razvojnih in testnih okolij z nižjimi stroški. Neprodukcijska verzija vključuje vse dodatne funkcije.

- Navideznost nam omogoča konsolidacijo številnih neizkoriščenih sistemov s heterogenimi aplikacijami in operacijskimi sistemi na en sam strežnik. Podobno lahko več navideznih naprav DataPower istočasno poganjamo na enem samem fizičnem strežniku.

Največja razlika med fizično in navidezno napravo je zahteva po konfiguraciji navideznih virov za navidezno napravo. Fizična naprava ima fiksno število procesorskih elementov, omrežnih kartic in delovnega pomnilnika. Namestitev navidezne naprave DataPower z dovolj procesorji, omrežnih in pomnilniških virov zahteva tehten premislek. Dodelitev prevelikega števila virov pripelje do neizkoriščenosti. Premalo virov pa do počasnih odzivnih časov, zavrnjenih zahtev in do nestabilnosti celotnega sistema.

V nadaljevanju dela bomo uporabljali fizično in navidezno napravo XI52 in se podrobneje lotili obremenjenosti procesorjev, omrežnih virov in pomnilnika za fizične in navidezne naprave DataPower. Dotaknili se bomo tudi nasvetov za konfiguracijo virov za navidezno napravo.

2.2 Uporaba naprave

Tipični primeri uporabe naprave DataPower so povečanje varnosti, nižanje stroškov, pohitritev delovanja in integracija različnih okolij. Na kratko bomo opisali vse.

2.2.1 Varnost

Visoko stopnjo varnosti lahko dosežemo zelo preprosto. Namestimo namensko napravo, ki ima omejen nabor funkcionalnosti, ki jih opravlja odlično. Naprave DataPower so narejene od spodaj navzgor z mislijo na varnost. Odstranjene so nepotrebne strojne komponente (npr. DVD-enota) in programske komponente (npr. telnet). Privzeto so vse funkcije izklopljene, tudi omrežni vhodi in administrativni pristopi, razen povezave preko serijskega vmesnika. Datotečni sistem je zakodiran. Skupnega datotečnega sistema ni. V primeru fizičnega posega v napravo, se bo le-ta izklopila in je ne bo več možno uporabljati. V tem primeru jo je potrebno poslati na uradni servis.

Naprava podpira specializirano delovanje z zasebnimi ključi in certifikati. Zasebnih ključev ni možno izvoziti iz naprave, razen pri generiranju ali z uporabo dodatnega modula. Naprava uporablja prilagojen operacijski sistem, ki je odporen na luknje v navadnih operacijskih

sistemih. Privzeto naprava zavrne vsa sporočila. Za vsako storitev moramo nastaviti kaj točno želimo sprejeti. Na razpolago imamo veliko možnosti za filtriranje, npr. IP-naslov, del HTTP-glave in vsebina sporočila.

Staro pravilo pravi, da se v DMZ zaključi povezava od klienta in da se iz varnega strežnika naredi povezava na zaledni sistem. Navadno imamo še bolj striktno varnostno politiko in želimo, da uporabniki opravijo prijavo in avtorizacijo pred povezavo na zaledne sisteme.

Pred uporabnikom želimo skriti samo implementacijo zalednih strežnikov in aplikacij. Tipični DMZ-produkti lahko skrijejo ime gostitelja, IP-naslov, vrata in URI. XML usmerjene naprave, kot je DataPower, lahko le-te skrijejo na bolj inteligentni ravni in naknadno nudijo analizo celotnega podatkovnega toka.

Poglavitni razlog za uporabo specializiranih naprav je, da lahko celoten sistem postane ogrožen zaradi XML-nevarnosti. Naprave tega tipa ponujajo prefinjene metode preverjanja. Izbiramo lahko med filtriranjem na osnovi podatkov znotraj sporočila, HTTP-paketa ali drugih omrežnih spremenljivk. Preverjamo lahko pravilnost sheme. Naprava nam omogoča zaščito pred XML- in XDoS-nevarnostmi. Zaščitimo se lahko pred spreminjanjem sporočila, XML-virusi in SQL-injekcijami.

2.2.2 Stroški

Zamislimo si primer, kjer za navidezni strežnik uporabimo programsko rešitev. Že za samo postavitev programskega posredovalnega strežnika bi potrebovali veliko različnih znanj, kar posledično pomeni višje stroške, ki jih lahko znižamo z namenskimi napravi. Z njimi so z administrativnega vidika značilnosti operacijskega sistema in datotečnega sistema nepomembne. Pri programski rešitvi je potrebna namestitev popravkov in novih verzij na vsaki ravni rešitve. Pri namenskih napravah tipično zgolj naložimo majhno strojno programsko opremo (angl. *firmware*) in naredimo posodobitev, ki je končana v nekaj minutah. Podobno je pri sami administraciji. Pri programski rešitvi imamo več konzol, tukaj pa samo eno.

Stroškov ne nižamo samo z namestitvijo in upravljanjem. Poglejmo primer, kjer imamo različne oddelke, ki uporabljajo spletne storitve na različnih okoljih, ti. Microsoft, Oracle in IBM. Podjetje ima lahko enotno varnostno politiko in SLM, ki mora biti implementirana na različna okolja. To je potrebno storiti za vsako okolje posebej, za kar potrebujemo ljudi z znanji za različna okolja. Konfiguracija se tako podvaja in je posledično dražja. Pri vsaki novi verziji lahko pride do težave, da okolja med seboj nimajo iste konfiguracije, kar lahko pripelje do izpada ali varnostnih lukenj.

Boljša rešitev bi bila implementacija naprave DataPower kot posredniškega strežnika za spletno storitev. Naložili bi potrebne WSDL datotek za vsako okolje in nato konfigurirali potrebne varnosti in SLM. Na ta način dobimo enotno točko za vsa okolja. Vse to postavimo na osnovi uveljavljenih standardov WS-Security, WS-Policy, WS-Addressing, WS-Management in WSDM.

2.2.3 Pospešitev delovanja

XML je postal osnova za večino modernih okolij. Razvil se je v SOAP za spletne storitve in ga najdemo skozi celotno širino in globino SOA. Do težav pri njegovi uporabi v smislu hitrosti in delovanja pride, ker je XML po obliki prijazen človeku in ne računalniku. Pretvorba v računalniku prijazno obliko zahteva omembe vredno obremenitev procesorjev in pomnilnika. Do tega pride zaradi pretvorbe XML dokumenta v pomnilniško obliko in preverjanja proti shema datoteki.

Razmislimo, kakšen vpliv imajo spremembe in preverjanja, ko imamo veliko količino XML/SOAP-dokumentov. Dodajmo še potrebo po varnosti, preverjanje identitete v LDAP-strežnikih, preverjanje digitalnega podpisa in dešifriranje podatkov. Za vse to potrebujemo velikansko količino virov in dragocenega časa, ki ga ne porabimo za poslovno logiko. Temu dodajmo še zapravljen čas, ko dobimo nepravilno formirane podatke ali podatke v nasprotju z varnostno politiko.

Z napredkom omrežne infrastrukture se je pojavil trend menjave namenske programske opreme z namensko strojno opremo, da bi povečali zmogljivosti. Podobno je prišlo do evolucije uporabe namenske strojne opreme za ponavljajoče XML-naloge, kot so sprememba podatkov, preverjanje pravilnosti shem in XSL-transformacije.

Protokoli, ki imajo za osnovo XML, ne vsebujejo vgrajenih varnostnih mehanizmov. SOAP skozi HTTP lahko pošlje občutljive podatke nezaščitene preko različnih omrežij. S pojavom standardov, ki rešujejo omenjeno težavo (WS-Security), je prišlo do povečanega bremena na kritične zaledne sisteme.

Naprava DataPower nam pomaga pri pospešitvi delovanja in sprostitvi virov na zalednih sistemih. Ko preverjamo digitalni podpis in izvajamo (de)šifriranje, pride do velike obremenitve procesorjev in pomnilnika na zalednih sistemih. Namenska XML-naprava pomaga premestiti breme iz zalednih sistemov in opravi naštete naloge v zelo kratkem času (skoraj pri hitrosti omrežnih povezav).

2.2.4 Integracija različnih okolij

Podpora za veliko število protokolov (HTTP, FTP, MQ, JMS, NFS, SNMP itd.) prinaša široke možnosti pri integraciji različnih okolij. Naprave DataPower lahko opravljajo transformacije ali XML v XML ali ne-XML v XML. Sporočila se lahko pretvorijo v format potreben za katerikoli zaledni sistem.

Če bi imeli infrastrukturo, ki deluje na zastarelih sistemih, npr. *mainframe*, in bi jo bilo potrebno povezati na novejše okolje, ki uporablja spletne storitve, bi bila preprosta rešitev da bi na obrobje omrežja, kjer bi delovala kot posredovalni strežnik (angl. *proxy*), namestili naprave DataPower. Narediti bi bilo potrebno še WSDL za opis spletnih storitev in že bi lahko sprejemali SOAP-sporočila. Konvertirali bi jih v COBOL Copybook in poslali preko MQ na zastarele zaledne sisteme, na katerih ne bi bilo potrebno spreminjati ničesar.

Pogosto se srečamo s potrebo po usmerjanju prometa na samem obrobju omrežja. Za to imamo DMZ-spletne strežnike, posredovalne strežnike in naprave za izenačevanje obremenitve (angl. *load balancers*). Težava z njimi je, da razumejo samo protokole in ne znajo razbrati vsebine sporočila. V tem primeru se običajno doda dodatno polje v HTTP-glavo, ki pomaga pri usmerjanju. Rešitev ni najboljša, ker lahko tako napadalcem razkrijemo del sporočila. Sama velikost HTTP-glave je omejena, kar nas dodatno omejuje pri rešitvi. SOA-namenske naprave razumejo XML-vsebino sporočila in lahko z uporabo XPath preverijo vsebino in se odločijo na podlagi vrednosti nekega elementa.

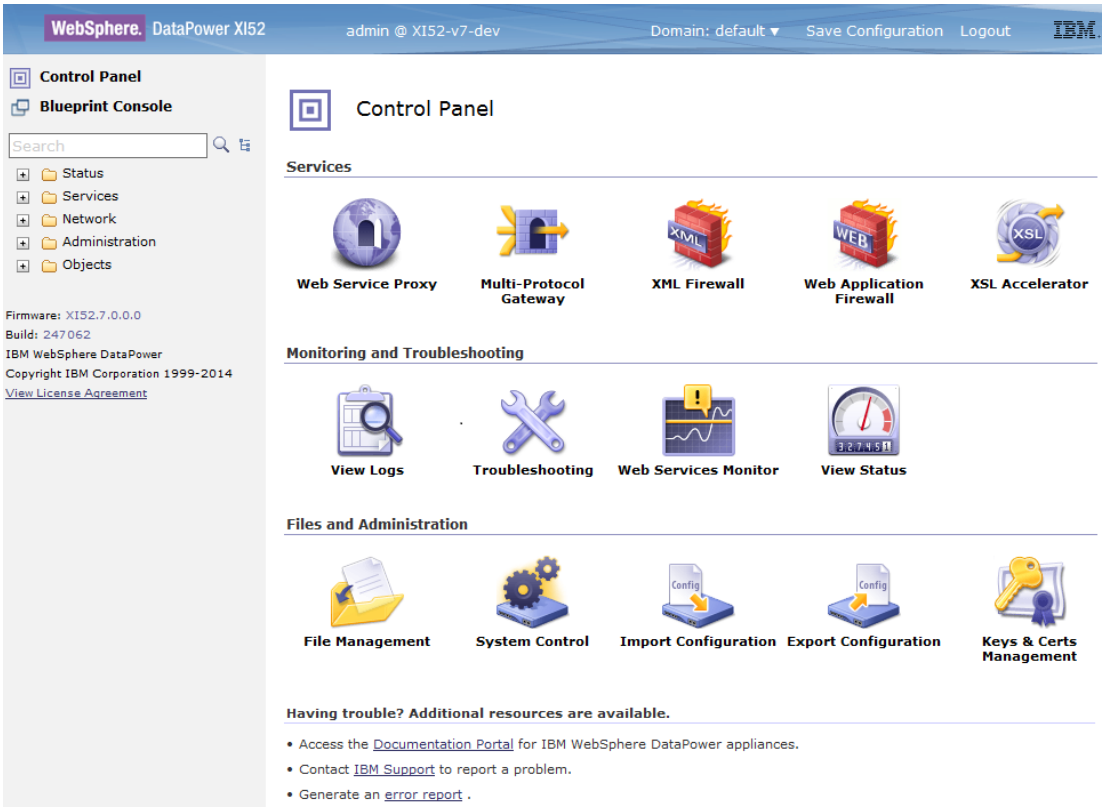
2.3 Upravljanje naprave

Vse na napravi DataPower je narejeno z mislijo na varnost. Iz tega razloga so privzeto vsi oddaljeni upravljalni pristopi onemogočeni. Edini način, da jih omogočimo, je preko serijskega vmesnika.

2.3.1 Načini upravljanja

Upravljanje naprave lahko izvajamo na več načinov.

- Dostop preko spletnega brskalnika je največkrat uporabljen način za administriranje naprave. V produkcijskih in zelo varovanih okoljih njena uporaba velikokrat ni dovoljena. Na sliki (slika 1) vidimo grafični vmesnik.



Slika 1: Grafični vmesnik

- CLI: Do njega lahko dostopamo preko že omenjenega serijskega vhoda in varne lupine (SSH). Administracija preko CLI je zelo podobna Cisco CLI, kar je običajno zelo domače skrbnikom omrežij. V sistemih z zelo visoko stopnjo varnosti so vsi oddaljeni dostopi onemogočeni. Edina možnost za konfiguracijo je fizični dostop v podatkovnem centru.

- XML upravljanje: Administratorjem omogoča dostop do naprave preko SOAP-sporočil. Obstaja več različnih specifikacij, ki jih lahko uporabimo, vključno z DataPower SOAP-upravljanjem konfiguracije, WS-Management in WSDM. Običajno uporabljamo upravljanje preko XML za avtomatizirano, programsko in prilagojeno administracijo.

2.3.2 Aplikacijske domene

Aplikacijske domene administratorjem omogočajo razdelitev naprave na logične enote. V produkciji lahko obstaja razdelitev na poslovne enote, npr. dobava in odprema. V razvojnem okolju pa vsakemu razvijalcu naredimo ločeno domeno. Konfiguracija v eni domeni je varna pred drugimi domenami, saj se med seboj ne vidijo. Na začetku ima naprava zgolj privzeto

domeno, v kateri naj bi nastavljali samo omrežne in administrativne nastavitve (IP, dostopi, NTP itd.). Domene nam omogočajo lažji prenos konfiguracije iz razvojnih okolij v testna, produkcijska. Olajšajo nam tudi sinhronizacijo med samimi napravami, npr. za potrebe visoke razpoložljivosti.

2.3.3 Faze konfiguracije

Obstajajo tri faze za namestitev in konfiguracijo naprave DataPower. Vsaka od njih vključuje različne tipe objektov in običajno jo zaradi ločitve vlog (razvijalec, administrator) izvede druga oseba v organizaciji.

- Namestitvena faza: Nastavimo različne objekte, ki nadzirajo omrežno konfiguracijo, usmerjanje, NTP in obvestila za kritične primere (nedelovanje omrežja, odpoved napajalnika itd.). Omenjene objekte nastavimo v privzeti domeni in so dostopne samo uporabnikom z administrativnimi pravicami. V času začetne konfiguracije bodo administratorji nastavili aplikacijske domene, uporabnike, skupine in pripadajočo varnostno politiko.

- Razvojna faza: Razvijalci in arhitekti pripravijo različne storitve, s katerimi bodo implementirali rešitve potrebne v njihovem SOA-okolju. Storitve lahko razvijejo na več načinov, odvisno od znanja. Čarovniki za pripravo omogočajo najhitrejši način kreiranja nove storitve in potrebnih objektov.

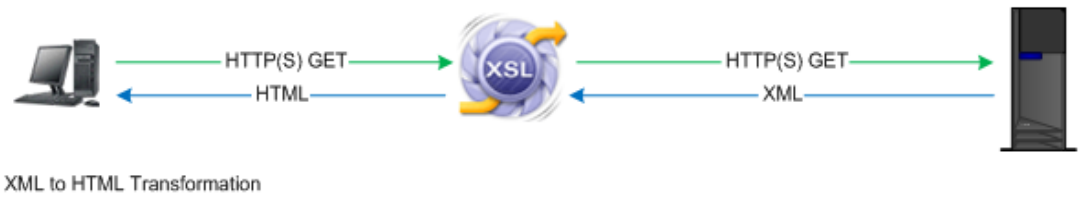
- Produkcijska faza: Že ime pove, da konfiguracijo namestimo v produkcijsko okolje. Naprava mora administratorjem omogočati nameščanje popravkov na redni osnovi. Omogočati mora tudi hiter, varen ter zanesljiv način namestitve nove konfiguracije ali verzije. Isto potrebujemo tudi za izvedbo varnostnih kopij. V tem koraku konfiguriramo tudi SNMP, monitorje in dnevnik sprememb.

2.4 Storitve

Za procesiranje prometa imamo na napravah DataPower na voljo več storitev. Na kontrolni plošči (slika 2) lahko izberemo med najbolj pogostimi storitvami, ki so:

Slika 2: Storitve na kontrolni plošči

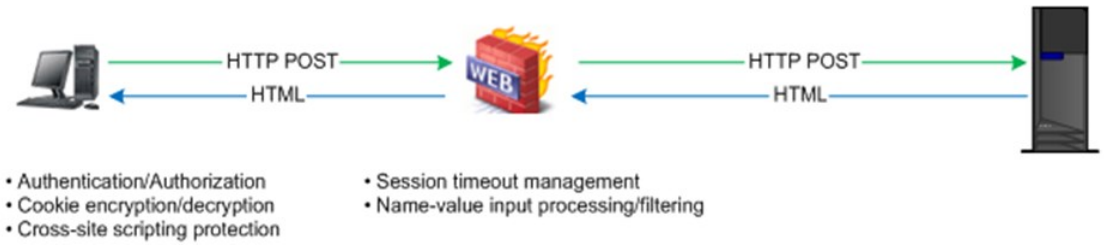
- XSL Accelerator: Pospeševalnik preverja in transformira vhodne ali izhodne XML-dokumente. Opravlja nalogo posredovalnega strežnika, naredi vsa potrebna preverjanja shem in transformacije na vhodnem sporočilu, predno ga pošlje na zaledni sistem. Za odgovore lahko opravi podobna preverjanja in transformacije z uporabo XSL.



Slika 3: XSL pospeševalnik

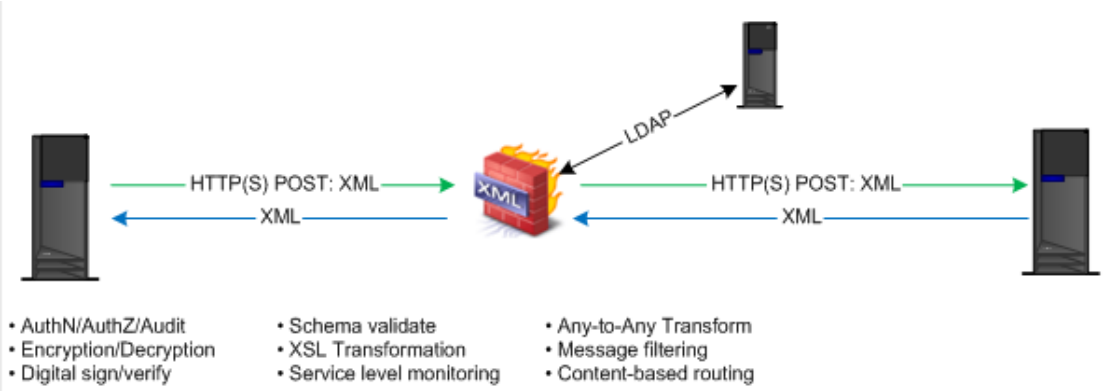
Uporabljamo ga lahko za pretvorbo iz XML v HTML, kot je prikazano na sliki 3. Uporabnik preko spletnega brskalnika pošlje zahtevo na spletno storitev. XSL-pospeševalnik ima vlogo posredovalnega strežnika med uporabnikom in zalednim sistemom. Zaledni sistem vrne navaden XML, ki se nato pretvori v HTML in vrne uporabniku.

- WAF: Narejen kot požarni zid za standardni HTML-promet, ki poteka skozi HTTP spletne aplikacije (slika 4). Poleg zaščite pred običajnimi nevarnostmi lahko požarni zid uveljavi specifično politiko na prometu med spletnim brskalnikom in zalednim sistemom. Primer, za dostop zahtevamo obstoj določenega piškotka.



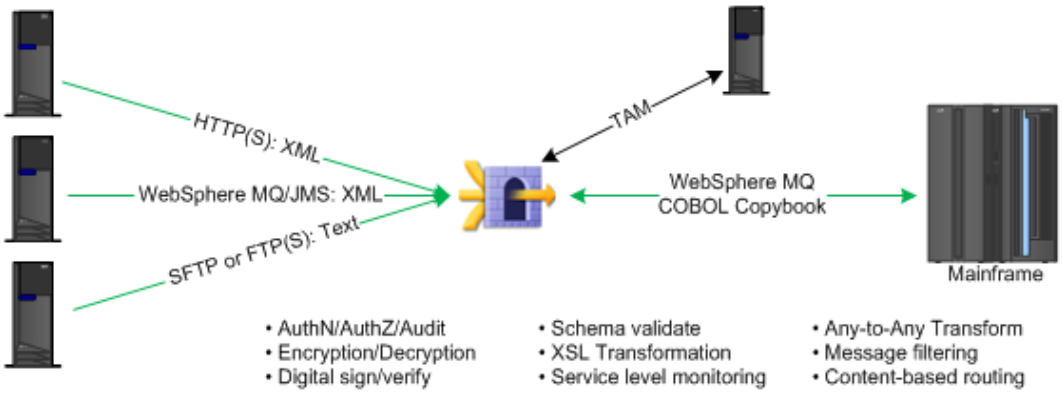
Slika 4: WAF

- XML Firewall: Splošno namenski požarni zid (slika 5) za HTTP- in HTTPS-storitve, ki lahko procesira tako XML- in kot tudi ne XML-podatke. Uporabimo lahko zelo širok nabor akcij na vhodnem in izhodnem prometu, šifriranje/dešifriranje, digitalno podpisovanje, XSL-transformacije, filtriranje, preverjanje pravilnosti sheme in dinamično usmerjanje. Privzeto je preverjanje za XML-nevarnosti.



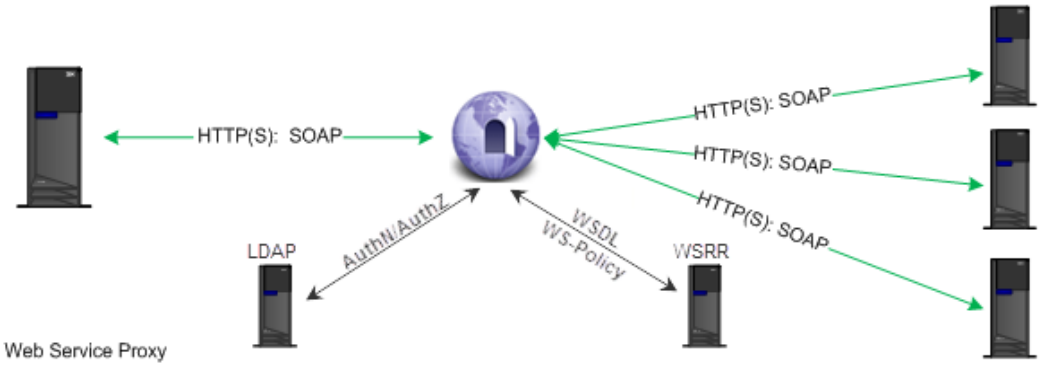
Slika 5: XML požarni zid

- MPGW: Predstavljajmo si ga kot razširitev XML požarnega zida s podporo za različne protokole (slika 6). Poleg že omenjenih HTTP in HTTPS deluje še z MQ, JMS, FTP, SFTP, NFS itd. Vse naštete protokole lahko med seboj povezujemo po želji. Primer: od uporabnika dobimo zahtevo preko HTTPS in jo usmerimo na MQ.



Slika 6: Večprotokolni prehod

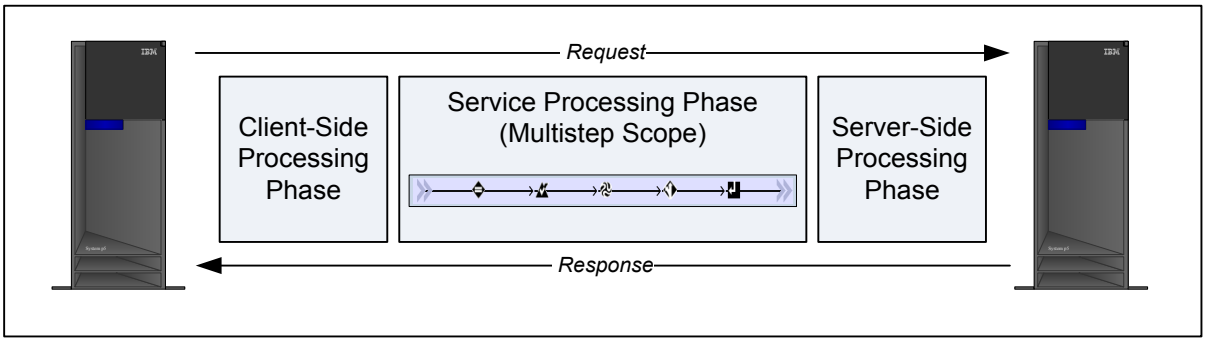
- WSP: Z njim lahko nastavimo enake funkcionalnosti kot pri večprotokolnem prehodu. Z uporabo enega ali več WSDL datotek omogoča dodatno avtomatsko konfiguracijo. Pridobimo jih lahko preko UDDI ali WSRR (slika 7). En posredovalni strežnik za spletne storitve je lahko enotna vstopna točka za več WSDL-datotek in opravlja avtomatsko usmerjanje prometa na zaželeni zaledni sistem.



Slika 7: Posredovalni strežnik za spletne storitve

2.5 Delovanje naprave

Storitev dobi zahtevo z določenega IP-naslova in vhoda. Preden je sporočilo poslano na zaledni sistem, sledi zaporedje dogodkov. Ločimo jih v tri faze (slika 8).



Slika 8: Faze procesiranja

1. Prejeto sporočilo bo usmerjeno na storitev, ki je konfigurirana za prejeto kombinacijo IP-naslova in vhoda. Ko storitev prejme zahtevo (npr. XML požarni zid), se porabi velik del časa, potrebnega za procesiranje sporočila. Npr. SSL-pogajanje in šifriranje podatkovnega toka, preverjanje SOAP-ovojnice, zaščita pred XML-nevarnostmi itd. Rezultati predprocesiranja lahko pripeljejo tudi do zavrnitve sporočila.

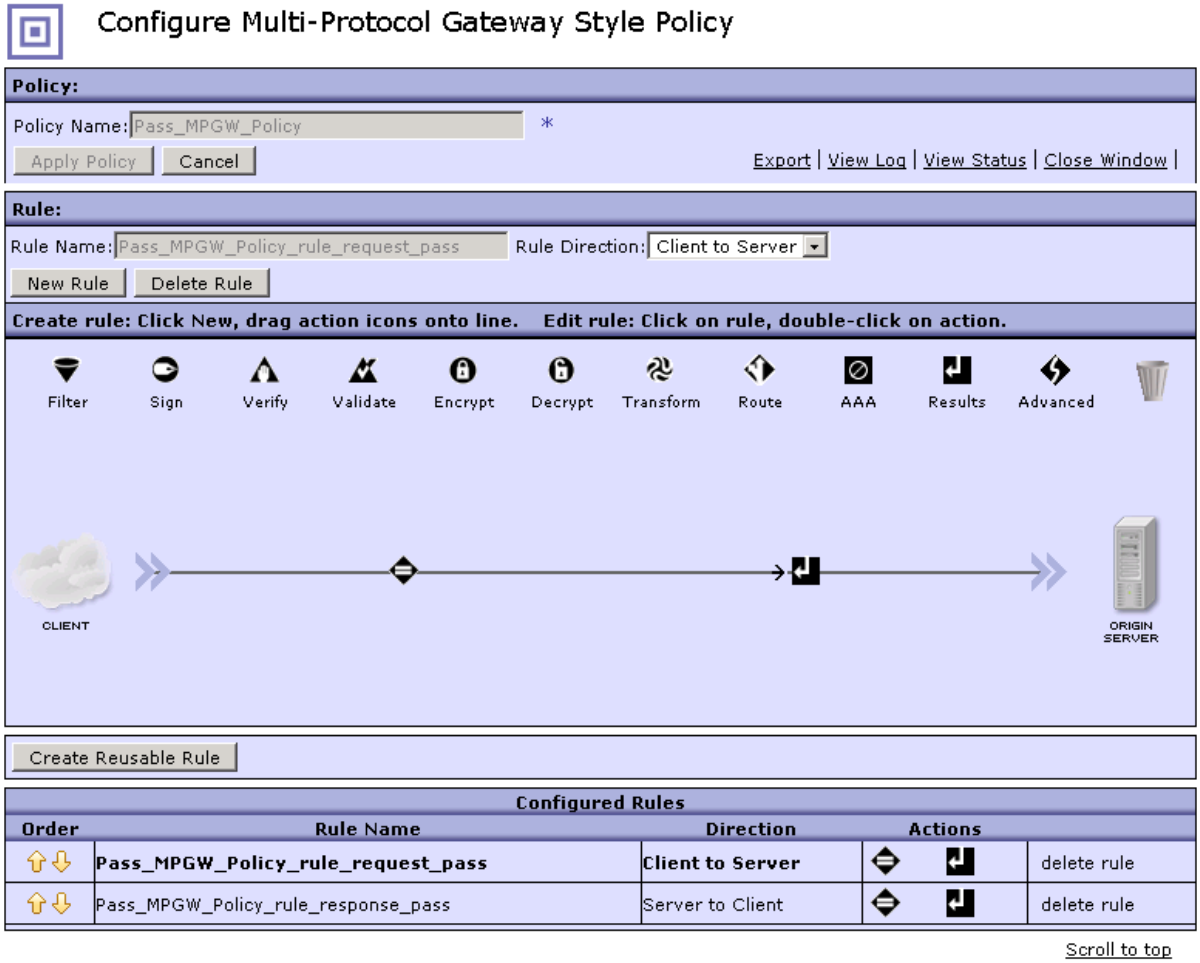
2. Po končanem vhodnem procesiranju in sprejetju sporočila, je le-to poslano v večstopenjsko procesiranje. Procesna politika je spisek pravil z določenimi akcijami, ki se lahko izvršijo nad vhodnim sporočilom. Akcije so določene operacije kot so šifriranje, digitalni podpis, preverjanje identitete itd. Ko sporočilo potuje skozi procesno politiko, se izvršijo akcije v določenem zaporedju in tako dobimo obliko, ki se pošlje zalednemu sistemu.

3. Po zaključku zgoraj omenjenih faz, je sporočilo pripravljeno za posredovanje na zaledni sistem, ta del imenujemo *strežniška faza procesiranja*. Običajno so potrebni še določeni koraki, preden se sporočilo pošlje. Npr. vzpostavitev SSL, nastavitev HTTP-glave, sprememba protokola (HTTP v JMS) itd.

Pri procesiranju odgovora se vse tri zgornje faze ponovijo z razliko, da je odgovor posredovan uporabniku. Za procesiranje odgovora imamo lahko različna pravila.

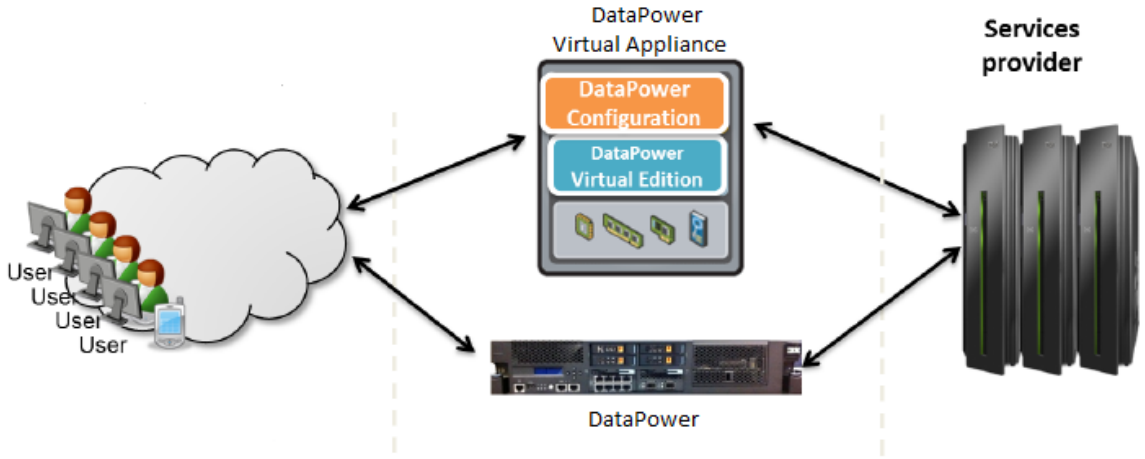
Poglavje 3 Opis testnega okolja

Scenarij uporabljen v diplomski nalogi prikazuje tipično uporabo varnostnega prehoda, in sicer možnost uporabe prehoda za dostop do različnih spletnih storitev v poslovnem procesu. Scenarij je narejen z uporabo večprotokolnega prehoda in se poslužuje osnovnih funkcionalnosti, ki jih omogoča naprava DataPower (varnost, preverjanje in transformacije). Slika 9 prikazuje primer večstopenjske politike MPGW v grafičnem vmesniku.



Slika 9: Primer večstopenjske politike MPGW

Slika 10 prikazuje topologijo okolja. Uporabniki, ki jih simuliramo z uporabo generatorja prometa (SoapUI [3]), pošiljajo zahteve na napravo DataPower. Naprava procesira sporočila in jih pošlje na zaledni sistem, aplikacijski strežnik WebSphere. Zaledni strežnik iz sporočila izlušči del podatkov in jih vrne nazaj na DataPower. Odgovor je procesiran z drugačno politiko kot zahteva. Povezava med uporabniki in DataPower je HTTPS, kar nam omogoča zaščito podatkov na ravni protokola. Uporabo virov na napravi DataPower bomo spremljali preko njenih vgrajenih funkcionalnosti.



Slika 10: Topologija okolja

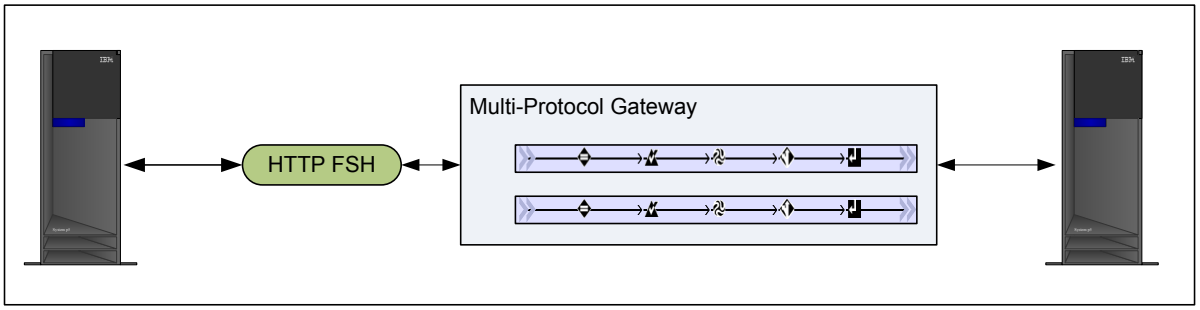
Slika 10 prikazuje dva scenarija z isto konfiguracijo. Razlika je v napravi DataPower. Prvi scenarij vsebuje navidezno napravo, drugi pa fizično napravo.

Okolje za simulacijo uporabnikov in zalednega sistema je postavljeno na VMware vSphere, verzija 5, z dvema strežnikoma IBM System x3850 X5, ki imata skupaj na voljo 159 GHz procesne moči in 255 Gb delovnega pomnilnika. Za simulacijo uporabnikov in postavitev zalednega sistema smo postavili navidezne strežnike Windows 2008 Standard R2. Vsaki navidezni in fizični napravi smo nastavili 10 Gb omrežni vhod, da smo minimizirali vpliv omrežja na testiranje, razen pri fizični napravi XI50, ki ima samo 1 Gb omrežne vhode. Okolje za navidezno napravo je postavljeno na VMware vSphere, verzija 5, z enim strežnikom IBM System x3650 M3, ki ima na voljo 37 GHz procesne moči in 45 Gb delovnega pomnilnika. Navidezni napravi DataPower smo spreminjali količino virov za potrebe testiranja, kot je razvidno v nadaljevanju. Uporabnike smo simulirali s programom SoapUI.

Vhodni podatek je preprosto SOAP-sporočilo velikosti 23 KB. Določena storitev na napravi najprej preveri, ali so vhodni podatki za njo, in temu sledijo konfigurirane akcije. V nadaljevanju si bomo ogledali podrobnejšo konfiguracijo.

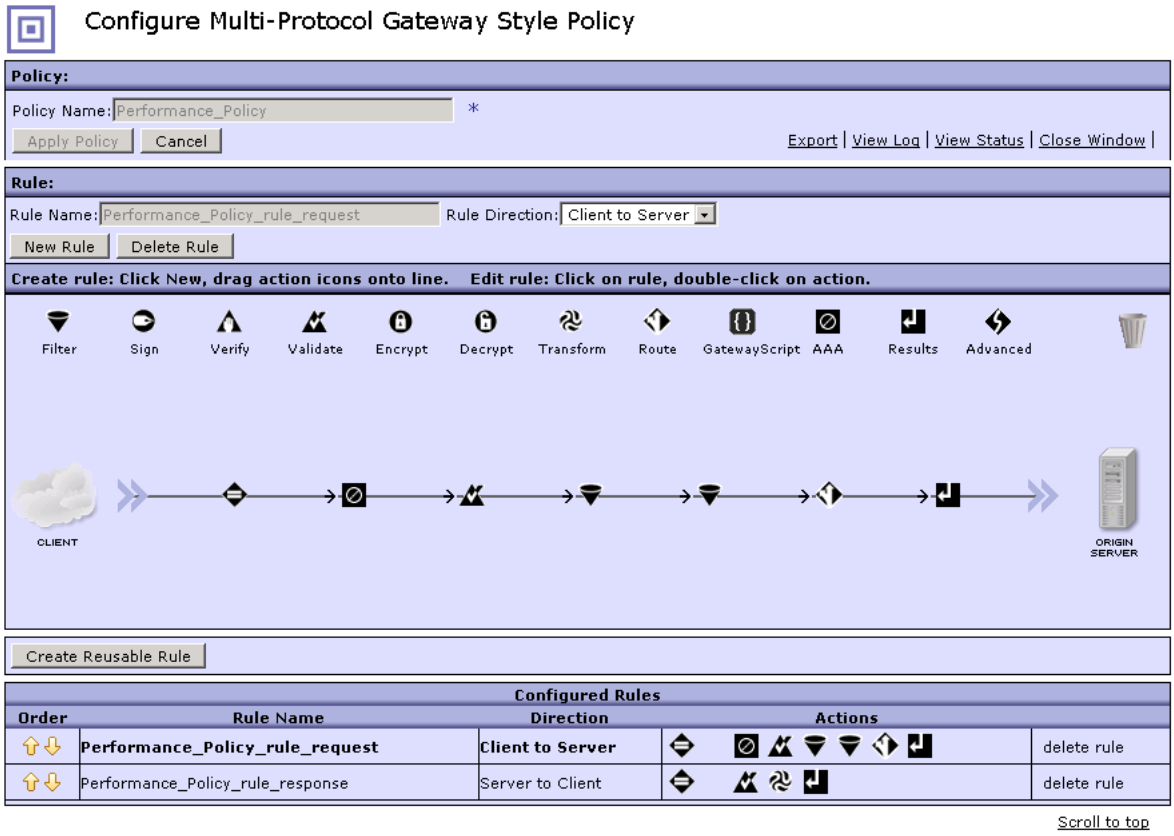
3.1 Konfiguracija MPGW

Pri konfiguraciji MPGW vnesemo osnovne informacije: ime, krajši opis ipd. Nato ustvarimo HTTPS-poslušalca, ki bo upravljal ves vhodni promet (slika 11).



Slika 11: Vhodni poslušalec

Sledi procesna politika s pripadajočimi pravili. Vsaka implementirana storitev ima lahko samo eno procesno politiko. Sestavljena je iz enega ali več pravil. Vsako se začne s primerjalno akcijo, ki ji sledijo ostale. Procesna pravila lahko veljajo za zahteve, odgovore, oboje ali napake. Pravilo, definirano za zahteve, ne bo upoštevano pri odgovoru. V kolikor nastavimo možnost v obe smeri velja, pravilo za zahteve in odgovore. Pravilo za napake se upošteva samo pri težavah, ki nastanejo pri procesiranju. Slika 12 prikazuje pravila, uporabljena v našem okolju.



Slika 12: Procesna politika in pravila

Opis pravila za uporabniške zahteve, kot ga vidimo na sliki 12 (akcije se vrstijo od leve proti desni):

- Vsako pravilo se začne s primerjalno akcijo, ki omogoča nastavitev primerjave na osnovi URL, HTTP-glave, HTTP-metode, napake in XPath. V našem primeru smo nastavili akcijo, ki je prestregla vsa sporočila; skozi to pravilo bodo šle vse možne kombinacije URL, odvisno od tega, ali gre za zahtevo ali odgovor.

- AAA-politika je skupek virov in procedur, ki nam omogočajo preverjanje, ali ima uporabnik pravico dostopati do določenih storitev, datotek itd. AAA-politika je filter za vhodno sporočilo. Sestavljena je iz sledečih akcij: pridobitev identitete in vira, preverjanje identitete, povezava identitete in virov, dodelitev pooblastil in revizije. Uporabili smo samo del njenih možnosti. Uporabnik pošlje prijavne podatke v HTTP-glavi. Primerjavo naredimo proti XML-datoteki na napravi DataPower za preverjanje identitete.

- XML-shema opisuje strukturo XML-dokumenta. Preverjanje sheme omogoča, da dosežemo pravilno, varno strukturo in vsebino sporočila. Preverjanje sheme štejemo med zahtevnejše operacije za procesor, kar za seboj potegne dodatne stroške. Zaradi tega razloga se velikokrat na zalednih sistemih izklopi preverjanje. Izpustitev preverjanja sheme se šteje med možne nevarnosti. Naprave DataPower omogočajo preverjanje oz. procesiranje s hitrostjo omrežja.

- Filtriranje na osnovi vsebine omogoča prilagojeno zaščito pred nevarnostmi. Prilagojeno filtriranje dosežemo z uporabo XSL-transformacije, v kateri definiramo, kdaj sporočilo zavrnemo oz. sprejmemo. Slika 13 prikazuje preverjanje sporočila, ali vsebuje besedo DataPower.

```
¶
<xsl:template match="/">↵
 → <xsl:choose>↵
 → → <xsl:when test="contains(//prod:brand,'DataPower')">↵
 → → → <dp:accept/>↵
 → → </xsl:when>↵
 → → <xsl:otherwise>↵
 → → → <dp:reject>Missing 'DataPower' trademark</dp:reject>↵
 → → </xsl:otherwise>↵
 → </xsl:choose>↵
</xsl:template>¶
¶
```

Slika 13: Filtriranje na osnovi sporočila

- Filtriranje pred SQL-nevarnostmi dosežemo na podoben način, kot pri zadnji opisani akciji, z uporabo XSL-transformacije. Težave nastanejo kadar imamo storitev, ki SQL-poizvedbo sestavi na osnovi uporabniškega sporočila. Storitev pričakuje SOAP-zahtevo z elementom last-name, s katerim sestavi SQL-poizvedbo, npr. iskanje stranke. V elementu imamo vrednost '1'='1', kar lahko pripelje do SQL-poizvedbe, ki bi vrnila spisek vseh strank.

- Dinamično usmerjanje na osnovi vsebine omogoča izbiro zalednega sistema glede na samo vsebino sporočila. V testu smo uporabili izbiro zalednega sistema s pomočjo XPath, v primeru vrednosti A pošlje sporočilo na strežnik A oz. v primeru vrednosti B na strežnik B. V samem testu je to pomenilo isti strežnik, kar pa nima vpliva na rezultate.

Opis pravila za odgovore iz zalednega sistema (akcije se vrstijo od leve proti desni): Primerjalna akcija deluje enako kot primerjalna akcija pri zahtevi. Preverjanje sheme deluje enako kot akcija preverjanje sheme pri zahtevi.

3.2 Spremljanje naprave in storitev

Kot večina omrežnih komponent tudi naprava DataPower spremlja storitve, porabo virov in jih prikazuje skozi različne metrike [4]. Med parametre, povezane na napravo, štejemo statistiko obremenitve procesorjev, porabo pomnilnika in datotečnega sistema in zasedenost omrežnih povezav.

Da ne bi prišlo do izpada, moramo vedno zelo podrobno spremljati celotno stanje naprave in njenih storitev. Specifičnost naprave, ki je posledica kompleksnega procesiranja, nas je pripeljala do treh načinov spremljanja:

- Splošno stanje spremljamo preko stanja strojne opreme, npr. temperatura, hitrost ventilatorjev in stanje napajalnih enot.
- Obremenitev sistema spremljamo z različnimi parametri, npr. obremenitev procesorjev, pomnilnika in datotečnega sistema.
- Pretočnost procesiranja lahko določimo z analiziranjem zasedenosti omrežnih povezav in števila transakcij.

Na napravah DataPower lahko spremljamo veliko različnih informacij, ki olajšajo pregled nad sistemom in njegovim stanjem. Najprej si oglejmo nekatere parametre za spremljanje splošnega stanja naprave:

- Z zasedenostjo sistema preverimo sposobnost naprave sprejeti dodatno breme. Osnova je formula, ki je sestavljena iz različnih komponent, npr. zasedenost procesorjev, pomnilnika in datotečnega sistema. To je tipično najboljša ocena za stanje sistema.
- Statistika obremenitve procesorjev je na voljo v petih različnih časovnih intervalih (10 sekund, 1minuta, 10 minut, 1 ura, 1 dan) in ni tako zanesljiva kot zasedenost sistema. Naprava DataPower ima zmožnost samo optimiziranja, kar lahko zaradi aktivnosti v ozadju privede do 100-odstotne zasedenosti procesorjev
- Statistika zasedenosti pomnilnika je na voljo za različne dele bliskovnega pomnilnika (angl. *flash memory*). Vidimo lahko odstotke zasedenosti in velikost celotnega pomnilnika.
- Na voljo imamo statistiko za prazen prostor in celoten prostor šifriranega, začasnega in internega datotečnega sistema. Ves čas moramo spremljati prostor, ki je še na voljo.

- Spremljanje omrežnih vmesnikov pove količino sprejetih in oddanih podatkov. Zasedenost nam pomaga tudi pri napovedi, kdaj bo prišlo do povečane obremenitve ali rasti prometa.

IT-storitve pogosto zahtevajo določeno stopnjo kvalitete v smislu odzivnega časa, pretočnosti in razpoložljivosti. Infrastruktura mora omogočati način spremljanja trenutnega stanja in možnost reagiranja v primeru nedoseganja določenih ciljev. Na napravi DataPower na eleganten način implementiramo storitve spremljanja. SLM omogoča spremljanje kritičnih točk, ki pomagajo prepoznati težave in odreagirati temu primerno. Cilj je doseči pričakovanja stranke za določeno storitev.

Z napravo DataPower lahko to dosežemo z uporabo naslednjih korakov:

- Nastavimo lahko filter za sporočilo, ki ustreza določenim pogojem.
- Določimo politiko za izbrana sporočila z uporabo merljivega intervala, praga in akcije, ki jo želimo izvesti.
- Uveljavimo lahko izbrano akcijo, če so doseženi izbrani pragovi.

Prednosti, ki jih dosežemo z uporabo SLM na napravi DataPower so:

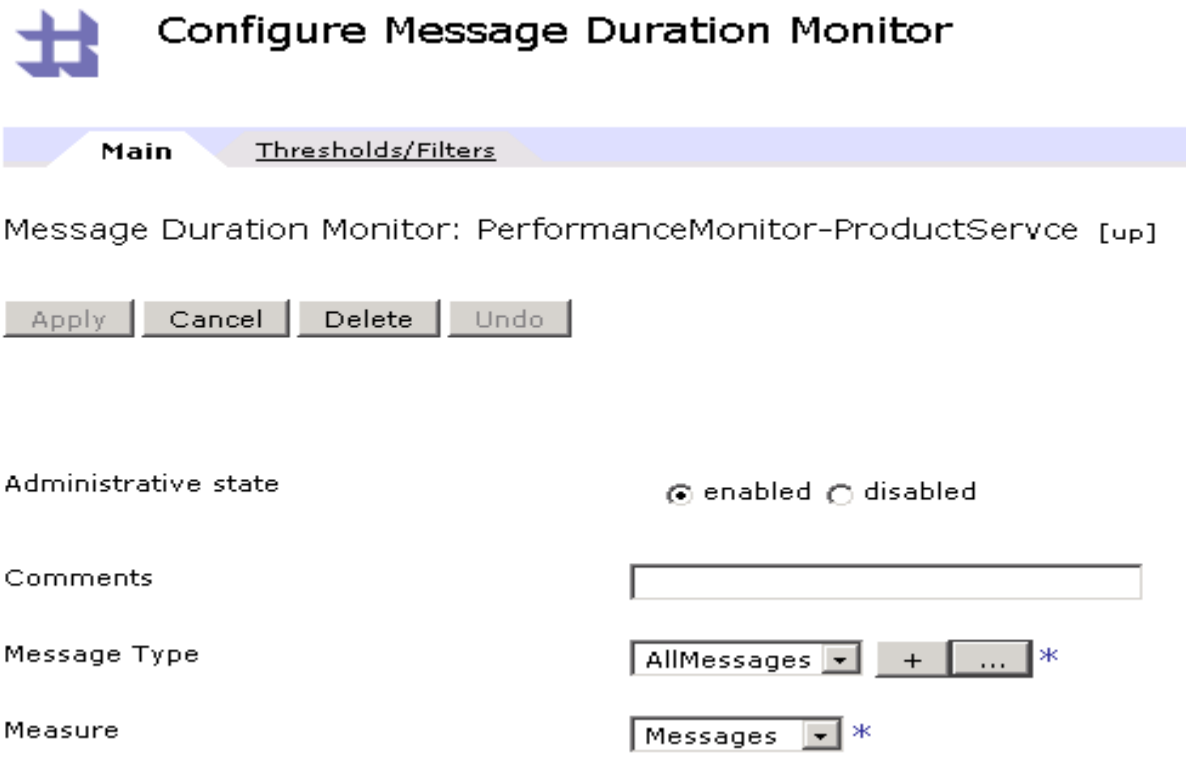
- Z uporabo SLM se izognemo zlorabi in preobremenjenosti storitev in jih zavarujemo pred ohromitvijo (DoS).
- Uveljavljamo lahko sporazume o ravni storitve (SLA).
- Razlikujemo med uporabniki glede na njihove potrebe oz. prioritete.
- Imamo možnost nastavitev akcij, kadar so doseženi določeni pragovi, npr. pošiljanje opozoril, če je prišlo do prevelikega števila nepravilnih sporočil.
- Optimiziramo odzivne čase in delimo vire med različne skupine uporabnikov, ki dostopajo do storitev.

Nastavimo lahko različne tipe, kot so spremljanje sporočil, spremljanje spletnih storitev in SLM-akcije. Spremljanje sporočil poteka med njihovim procesiranjem z uporabo pragov in akcij. Poznamo dva tipa: spremljanje števila in spremljanje časa.

Pri spremljanju števila sporočil (štejemo število sporočil v določenem časovnem intervalu) in v primeru preseženega praga lahko izvedemo določeno akcijo (pošljemo obvestilo, zavrnemo sporočilo).

Pri spremljanju časa, merimo potreben čas za procesiranje sporočila. Nastavimo lahko interval, potreben za obdelavo zahteve, odgovora ali obojega. Lahko izmerimo tudi čas, ki ga je potreboval zaledni sistem za vrnitev odgovora.

V našem primeru bomo spremljali zasedenost sistema, statistiko obremenitve procesorjev, zasedenosti pomnilnika, število zahtev na sekundo. Na sliki 14 imamo konfiguracijo za merjenje časa pri procesiranju sporočila.



Slika 14: Konfiguracija merjenja časa pri procesiranju sporočila

Poglavje 4 Analiza in predlogi za optimizacijo navidezne naprave

Scenarij uporabljen v diplomskem delu predstavlja običajen primer uporabe naprave DataPower. Prikazuje dostop do spletnih storitev v poslovnem okolju. Bremena smo simulirali z uporabo programa SoapUI, ki omogoča simulacijo velikega števila uporabnikov in podatkov. Uporabniki so pošiljali SOAP-sporočila preko HTTPS protokola na izbrani vhod. Podatke obremenjenosti sistema, procesorjev in pomnilnika smo zbirali s pomočjo CLI-ukazov (*show load, show memory in show cpu*) in grafičnega vmesnika. Rezultati so bili zajeti v določenih intervalih (na vsakih 600 sekund). Zasedenost sistema je rezultat povprečja zbranih vrednosti. Pri zasedenosti pomnilnika je namesto povprečne vrednosti vzeta najvišja vrednost. Ko zasedenost pomnilnika preseže določeno vrednost, začne naprava zavračati zahteve in tako varčevati z viri [5 ,6].

4.1 Testni scenariji

Uporabljena konfiguracija za vse testne scenarije je opisana v poglavju 3. Testirali smo navidezno napravo z različnim številom procesorjev, začeli smo s 4 procesorji in nadaljevali z 8, 16, 20 in 24 procesorji. Tabela 1 prikazuje različne konfiguracije navidezne naprave, uporabljene v testu. Za primerjavo smo testirali še fizično napravo DataPower XI50 in XI52.

Navidezna DataPower naprava					
Število procesorjev	4	8	16	20	24
Delovni pomnilnik (Gb)	4	8	8	8	8

Tabela 1: Konfiguracija navidezne naprave

Namestitev s 4, 8 in 16 procesorji je predpripravljena konfiguracija za navidezne naprave. Imenujemo jih majhna, standardna in velika. Majhna konfiguracija zahteva 4 procesorje in 4 Gb delovnega pomnilnika. To je s strani IBM tudi najmanjša podprta konfiguracija. Različno količino pomnilnika (tabela 1) bomo pojasnili v nadaljevanju.

Z uporabo že omenjenega programa SoapUI smo generirali konstantno obremenitev. Simulirali smo istočasno delovanje 9999 uporabnikov.

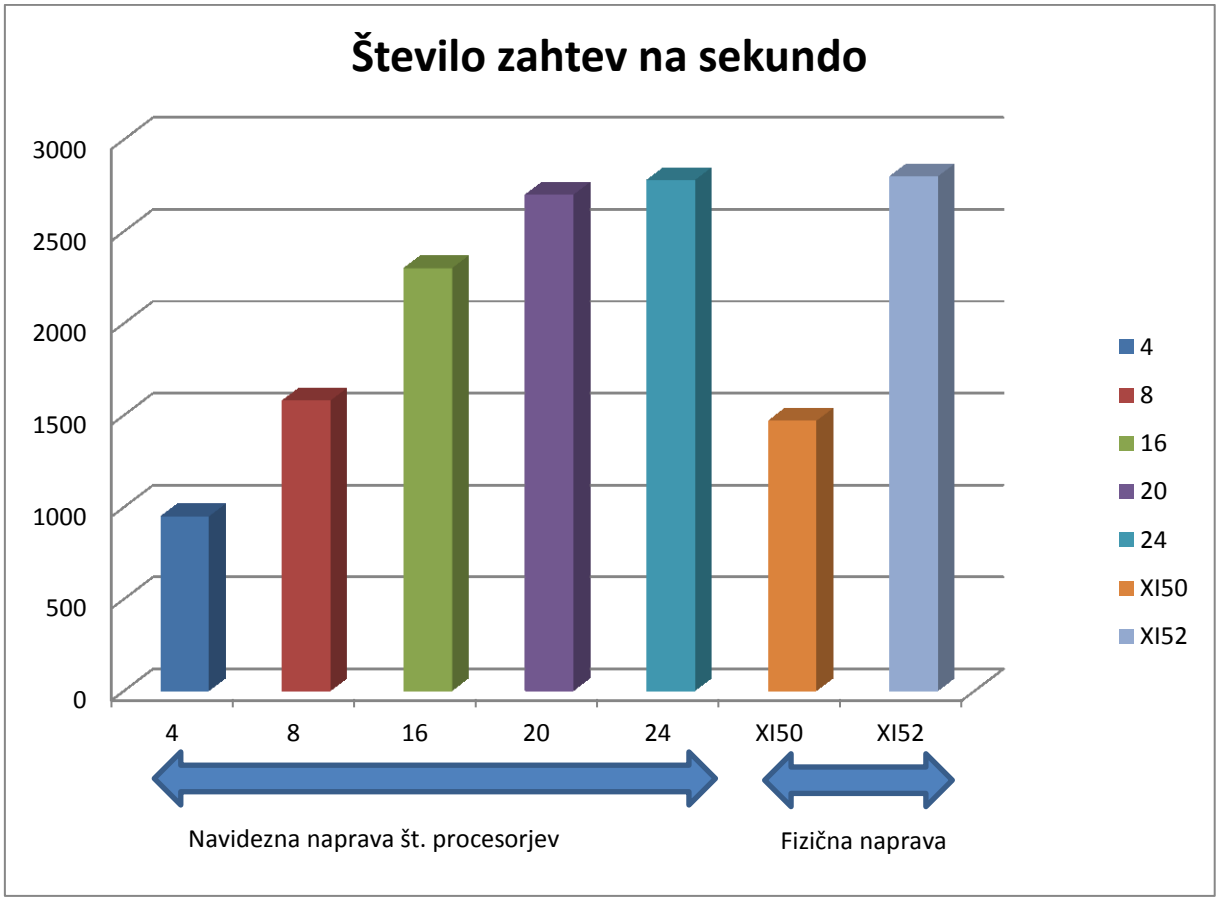
4.2 Rezultati merjenja

Testi so bili izvedeni v kontroliranem laboratorijskem okolju. Rezultati zmogljivostnih testov so lahko zelo različni, odvisni od scenarija, strojne opreme in ostalih parametrov. Podatki podani v diplomskem delu so nam v pomoč pri splošnih napotkih za načrtovanje virov za navidezno napravo.

naprava DataPower	število transakcij na sekundo	zasedenost sistema	obremenitev procesorjev	zasedenost pomnilnika
Navidezna 4	950	100%	99%	2,60 Gb
Navidezna 8	1580	100%	99%	3,20 Gb
Navidezna 16	2300	100%	99%	3,25 Gb
Navidezna 20	2700	89%	89%	3,36 Gb
Navidezna 24	2780	83%	75%	3,40 Gb
Fizična XI50	1470	100%	99%	1,84 Gb
Fizična XI52	2800	88%	83%	2,88 Gb

Tabela 2: Rezultati testiranja

Rezultati testiranja so prikazani v tabeli 2. Vsi testi so bili izvedeni z uporabo varnostnega protokola HTTPS med uporabniki in napravo DataPower. Slika 15 na navpični osi prikazuje maksimalno doseženo število zahtev na sekundo v odvisnosti od števila procesorjev na navidezni in fizični napravi.

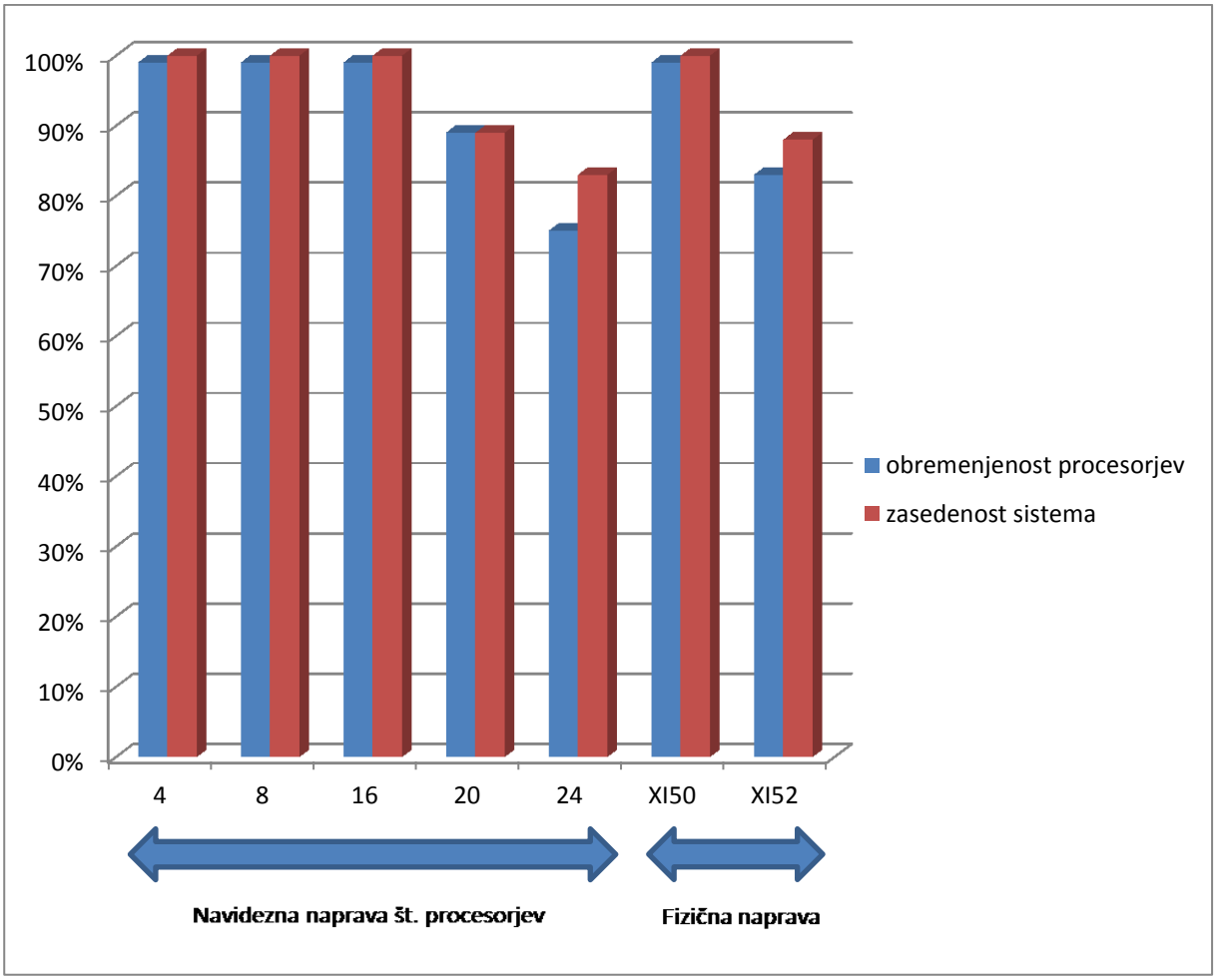


Slika 15: Število zahtev na sekundo

Rezultati kažejo, da imata fizična naprava XI52 in navidezna naprava s 24 procesorji skoraj enake zmogljivost. Predhodnik XI50 doseže približno 52 % zmogljivosti novejše naprave. Rezultati za navidezno napravo so prikazani z različnim številom procesorjev. Meritve smo opravili s 4, 8, 16, 20, 24 procesorji. Opravili smo še meritve za navidezno napravo XG45, ki pa jih nismo vključili med rezultate.

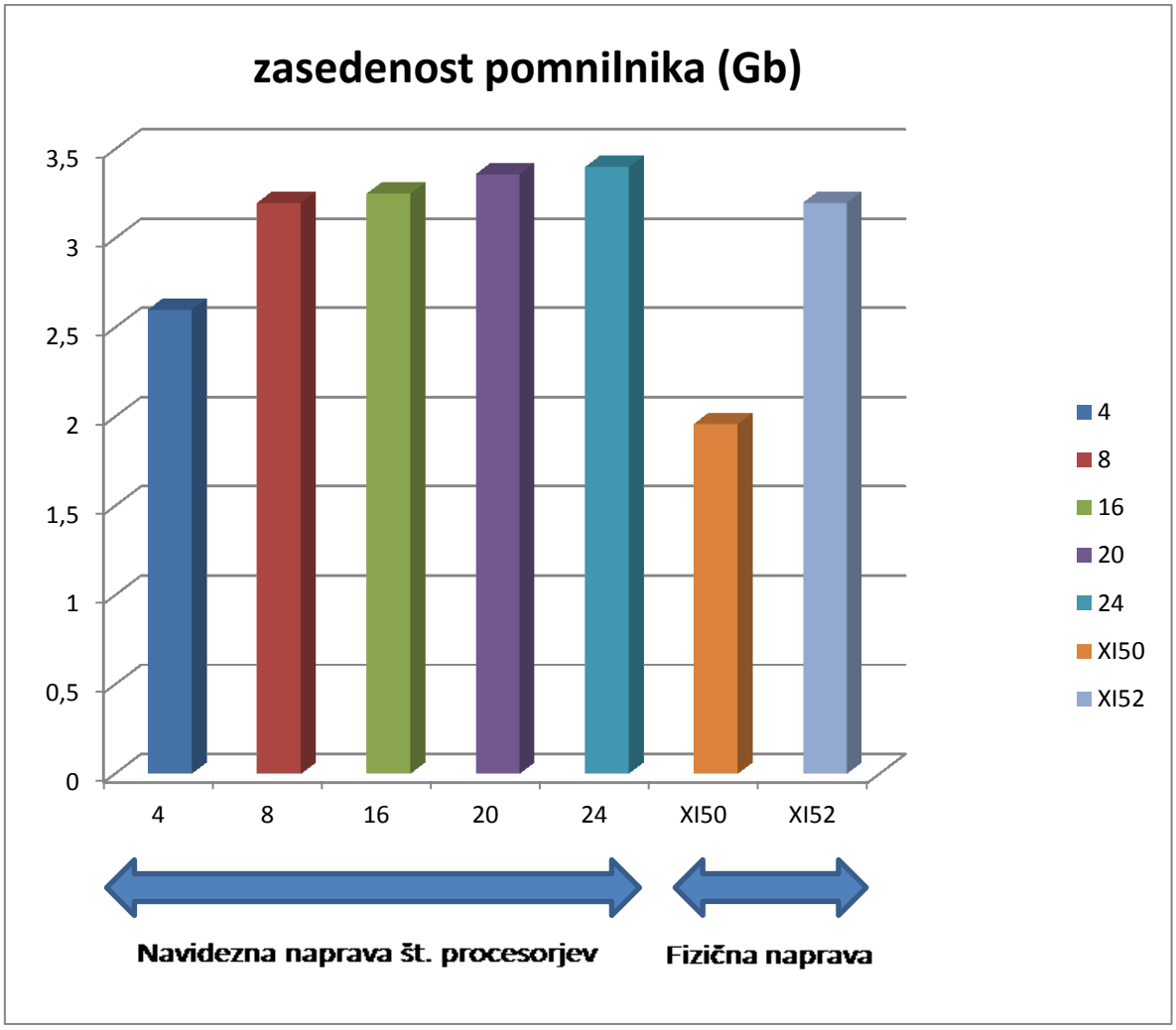
Na sliki 16 vidimo veliko izboljšanje pri prehodu 4 na 16 procesorjev. Pri številu 20 smo skoraj dosegli fizično napravo XI52 (prišli smo na 96 odstotkov). Pri številu 24 smo fizično napravo dohiteli, ampak z zgolj zanemarljivo razliko.

Slika 16 prikazuje obremenitev procesorjev. S slike je razvidna povezava med zasedenostjo sistema in obremenitvijo procesorjev.



Slika 16: Zasedenost sistema in procesorjev

Na sliki 17 vidimo največjo porabo pomnilnika v času testiranja. V našem scenariju je bilo 4 Gb pomnilnika dovolj samo pri 4 procesorjih. Za vse ostale konfiguracije smo morali uporabiti 8 Gb pomnilnika. Naprava DataPower začne pri 80-odstotni zasedenosti pomnilnika zahteve zavračati.



Slika 17: Največja zasedenost pomnilnika

4.3 Izsledki

Pri namestitvi navidezne naprave moramo nastaviti tri ključne vire:

- Nastaviti moramo število navideznih procesorjev.
- Nastaviti moramo količino delovnega pomnilnika za procesiranje zahtev in odgovorov.
- Konfigurirati moramo omrežne vhode, število le teh je v naprej določeno na 4.

Konfiguracija diskovne kapacitete nima omembe vrednega vpliva na delovanje same naprave.

4.3.1 Konfiguracija navideznih procesorjev

Najmanjše podprto število procesorjev je 4. Navidezna naprava bo načeloma delovala tudi z manj procesorji, vendar bomo v dnevniku videli zapise napak. Za dosego visoke pretočnosti sistema je predlagana konfiguracija 16 procesorjev, kar je tudi privzeta nastavitev za visoko zmogljiva okolja (angl. *enterprise configuration*).

Za večjo zmogljivost lahko nastavimo večje število procesorjev. Iz prej omenjenih podatkov je razvidno, da ne pridobimo, kolikor porabimo (količina dodatnih virov in dodatne licence). Boljša rešitev je namestitev dodatnih navideznih naprav v skupino za izenačitev bremena (angl. *load balancing group*). V tem primeru več naprav povežemo med seboj z uporabo dodatka Application Optimization. Ena izmed naprav postane vodja (angl. *master*) in porazdeli breme med vsemi napravi v skupini. Omenjene naprave so lahko nameščene na isti ali ločeni strojni opremi, odvisno od virov, ki so nam na voljo.

Iz podatkov našega testiranja je razvidno, da lahko fizično XI50 napravo nadomestimo z namestitvijo navidezne naprave z 8 procesorji, ob predpostavki, da imamo na voljo približno isto strojno opremo kot v našem scenariju. Fizično napravo XI52 bi skoraj lahko nadomestili z navidezno napravo s 16 procesorji. V okoljih z manjšo obremenitvijo, razvojnih in testnih običajno navidezne naprave namestimo s 4 do 8 procesorji.

Pri navidezni napravi s premalo procesorjev bo obremenitev le-teh konstantno visoka. naprava DataPower je zasnovana z mislijo na visoko obremenitev in bo običajno delovala stabilno ter zanesljivo. Bo pa visoka obremenitev procesorjev pripeljala do daljšega odzivnega časa. V skrajnem primeru lahko pride do prekinitve delovanja zaradi časovnih omejitev.

4.3.2 Konfiguracija delovnega pomnilnika

Količina nastavljenega delovnega pomnilnika nam določi število zahtev, ki bodo procesirane vzporedno. Najboljša metoda za določitev potrebnega pomnilnika je, da preverimo največjo porabo v okolju s fizično napravo. Tudi po namestitvi navidezne naprave moramo redno spremljati porabo pomnilnika.

V pomoč pri določitvi pomnilnika nam je tudi število zahtev in velikost sporočil. Za vsako zahtevo in odgovor bo naprava rezervirala določen del pomnilnika potreben za izvedbo vseh akcij. Pri XSLT-transformacijah bo naprava vhodne podatke spremenila v drugačne izhodne podatke, kar moramo upoštevati pri samem izračunu porabe pomnilnika. Potrebujemo prostor

za vhodne in tudi za obdelane podatke. Zagotoviti moramo prostor, ki ga bo potrebovala vsaka akcija.

Naprava DataPower se najbolje obnese, ko zasedenost pomnilnika ne preseže 80 %. Privzeto bo naprava začela zavračati zahteve, ko presežemo omenjeno vrednost. V primeru, da presežemo 80 %, imamo možnost nastaviti izravnalnik (angl. *buffer*) za 500 zahtev. V obeh primerih imamo ali nedosegljivo storitev ali pa povečan odzivni čas. Čeprav omejimo porabo, lahko pride do popolne izrabe pomnilnika in v skrajnem primeru do samodejnega ponovnega zagona naprave.

Nastavitev zadostne količine pomnilnika na navidezni napravi je zelo pomemben del upravljanja. Upoštevati pa moramo tudi omejitve strojne opreme. Količina navideznega pomnilnika nikoli ne sme preseči količine fizičnega pomnilnika, sicer bo do razbremenitve fizičnega pomnilnika prišlo s pisanjem na disk (angl. *swapping*). Posledično bomo imeli slabe odzivne čase ali celo neodzivno okolje.

4.3.3 Konfiguracija omrežnih vhodov

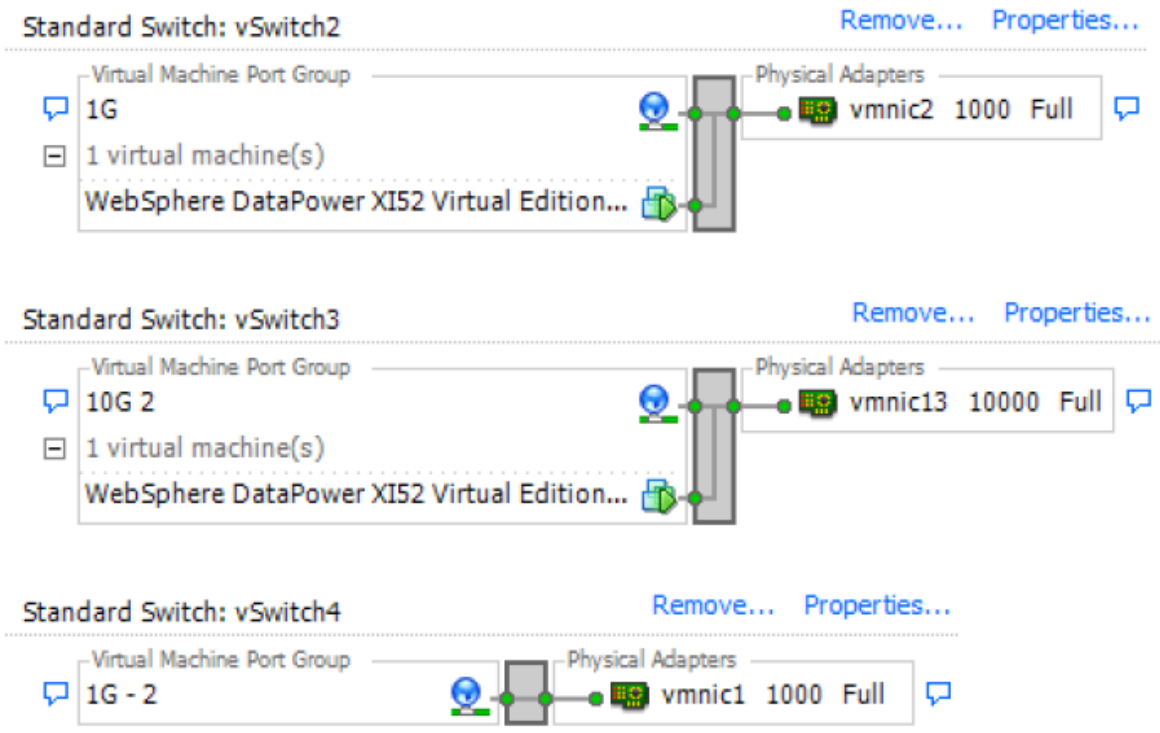
S številom konfiguriranih omrežnih vhodov nadzorujemo možno količino podatkov, ki jih lahko naprava DataPower obdela.

Število vhodov je odvisno od naprave. Poglejmo razlike:

- Fizična naprava XI50 ima 3x 1 Gb omrežni vhod in 1 vhod za upravljanje.
- Fizična naprava XI52 ima 2x 10 Gb in 8x 1 Gb omrežni vhod. Polega tega ima še 2x 1 Gb vhoda za upravljanje.
- Navidezna naprava podpira 4 omrežne vhode, ki so lahko 1 Gb ali 10 Gb.

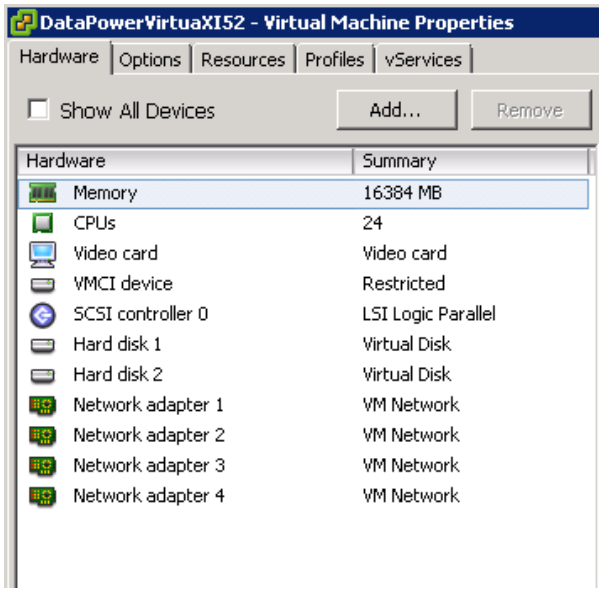
Število potrebnih fizičnih omrežnih vhodov lahko določimo z upoštevanjem velikosti zahteve in odgovora, ki bo potovala skozi določen navidezni omrežni vhod. 1 Gb omrežni vhod prenese približno 100 MB podatkov na sekundo. V našem primeru to pomeni približno največ 4500 zahtev na sekundo.

Pomembno je, da preslikamo navidezno omrežno kartico v fizično omrežno kartico, v kolikor potrebujemo celotno zmogljivost fizičnega vhoda. Na sliki 18 vidimo primer omenjene konfiguracije.



Slika 18: Primer konfiguracije omrežnih vhodov

Navidezna naprava s premalo omrežnih virov nas bo privedla do daljših odzivnih časov ali celo do časovnih omejitev. Omrežja običajno z lahkoto prenesejo veliko obremenitev in ostanejo stabilna, vseeno pa lahko pride do izgube paketov in potrebe po ponovitvi pošiljanja. Na sliki 19 vidimo primer konfiguracije navidezne naprave.



Slika 19: Primer navidezne naprave

Poglavje 5 Zaključek

V diplomskem delu smo podali splošen pregled zmogljivosti in porabe virov na napravah DataPower. Pri navidezni napravi smo opazili občutne izboljšave pri prehodu iz 4 na 16 procesorjev. Navidezna naprava ima lahko isto zmogljivost kot fizična naprava. Opazili smo, da je boljša rešitev več navideznih naprav kot ena sama z velikim številom procesorjev.

Pri namestitvi navideznih naprav je potrebno zelo dobro načrtovanje virov. Pozorni moramo biti na obremenitev procesorjev in delovnega pomnilnika. Zelo pomemben je pomnilnik, saj nas premalo pomnilnika v skrajnem primeru lahko pripelje do samodejnega ponovnega zagona.

Podani podatki so nam v pomoč pri namestitvi navidezne naprave, ko imamo opravka s podobno konfiguracijo storitve kot v našem primeru. Testiranje bi lahko razširili na druge storitve. Primerjali bi lahko transformacijo podatkov iz binarne oblike v XML in obratno. Testirali bi lahko tudi pretvorbo med različnimi protokoli in naredili primerjavo z izdelki konkurenčnih proizvajalcev.

Literatura

[1] International Technical Support Organization, IBM WebSphere DataPower SOA Appliances Part I: Overview and Getting Started, REDP, 2008

[2] Bill Hines et al., IBM WebSphere DataPower SOA Appliance Handbook, IBM Press, 2008

[3] SoapUI [Online]. Dosegljivo: http://www.soapui.org (dostop september 2014)

[4] International Technical Support Organization, IBM WebSphere DataPower SOA Appliances Part IV: Management and Governance, REDP, 2008

[5] Optimizacija zmogljivosti [Online]. Dosegljivo: http://www.ibm.com/developerworks/webservices/library/ws-dpperformance/index.html (dostop september 2014)

[6] Spremljanje naprav [Online]. Dosegljivo: http://www.ibm.com/developerworks/websphere/library/techarticles/1003_rasmussen/1003_rasmussen.html (dostop september 2014)